The Group of Isomorphisms of an Abelian Group and Some of its Abelian Subgroups.

By G. A. Miller.

§ 1. *Introduction.*

Let G represent any abelian group, while I represents its group of isomorphisms. It is known that a necessary and sufficient condition that I be abelian is that G is cyclic. Moreover, the invariant operators of I are composed of those which transform every operator of G into the same power of itself, and hence the order of the central of I is $\phi(m)$, m being the largest order of an operator contained in G.* In the present paper we aim to determine a few new properties of I, especially as regards its Sylow subgroups. This paper has close contact with an article by the same author entitled "Isomorphisms of a Group whose Order is a Power of a Prime," *Transactions of the American Mathematical Society*, Vol. XII (1911); and a paper by Burnside entitled "On Some Properties of Groups whose Orders are Powers of Primes," *Proceedings of the London Mathematical Society*, Vol. XI (1912).

Let A_0 represent any abelian subgroup of I. All the operators of G which are invariant under one of the operators of A_0 constitute an invariant subgroup under each one of the operators of A_0. If t_1 and t_2 are any two operators of A_0 while s is any operator of G, there result equations of the form:

$$t_1^{-1}st_1=s_1s, \quad t_2^{-1}st_2=s_2s, \quad t_1^{-1}s_2t_1=s_1^1s_2,$$

where s_1, s_2 and s_1^1 are also operators of G. Since $t_1t_2=t_2t_1$, there result the following equations:

$$t_2^{-1}t_1^{-1}st_1t_2=t_2^{-1}s_1t_2s_2s=t_1^{-1}t_2^{-1}st_2t_1=s_1^1s_1s_2s.$$

As $t_2^{-1}s_1t_2=s_1^1s_1$, we have the theorem: *If any two commutative operators t_1 and t_2 of the group of isomorphisms of an abelian group G transform a given*

* *Transactions of the American Mathematical Society*, Vol. II (1901), p. 260; cf. Ranum, *ibid.*, Vol. VIII (1907), p. 84.

operator of G into itself multiplied by s_1 and s_2 respectively, then the commutator of t_1 and s_2 is equal to the commutator of t_2 and s_1. On the other hand, it is easy to see that t_1 and t_2 must be commutative whenever these commutators are equal, so that the given condition is a sufficient as well as a necessary condition that t_1 and t_2 be commutative, provided s may represent any operator of G.

As a special case of the theorem of the preceding paragraph, it may be observed that every subgroup of I which is composed of operators transforming all the operators of G into themselves multiplied by operators which are invariant under all the operators of this subgroup is necessarily abelian, but an abelian subgroup of I is not always composed of such operators. The commutators of G whose elements are composed of a particular operator t of I and of all the operators of G, taken successively, constitute a subgroup T of G which may be associated with t.* In this way every operator of I may be associated with a particular subgroup of G. The identity of I is the only operator in I which corresponds to the identity of G, but the subgroups of G which correspond to other operators of I are not necessarily distinct when these operators are distinct. On the other hand, two operators of I are clearly distinct whenever their associated, or corresponding, subgroups are distinct.

The subgroup of G which is associated with t^{α} is clearly contained in T for every value of α. The subgroups of G which correspond to the operators of any cyclic subgroup of I must therefore all be contained in each of the subgroups which correspond to the generators of this cyclic subgroup of I. In particular, I involves at least two operators which correspond to the same subgroup of G whenever I involves an operator whose order exceeds 2. If G is the cyclic group of order 12, it is evident that any two distinct operators of I correspond to two distinct subgroups of G; but if G is an abelian group which is not contained in this cyclic group, then the I of G cannot have the property that every pair of its distinct operators corresponds to a pair of distinct subgroups.

When T is composed of operators which are invariant under t, the order of t is the same as the largest order of an operator of T, and the subgroup of G which corresponds to t^{α} is composed of the α-th power of the operators of T. Since the group of isomorphisms of any abelian group is the direct product of the group of isomorphisms of its Sylow subgroups, we may confine ourselves to a study of the case when the order of G is a power of a prime number.

---

* *Bulletin of the American Mathematical Society*, Vol. VI (1900), p. 337.

§ 2. *Order of G is p^m, p being any Prime Number.*

We shall first determine the order of a Sylow subgroup of order $p^{m'}$ in the group of isomorphisms of any abelian group of order p^m, p being any prime number. Suppose that the independent generators of G are of orders p^{α_1}, p^{β_1}, $\ldots$, p^{λ_1} $(\alpha_1>\beta_1>\ldots>\lambda_1)$, and that the number of the independent generators of these orders is α, β, $\ldots$, λ respectively. Hence

$$m=\alpha\alpha_1+\beta\beta_1+\ldots+\lambda\lambda_1.$$

It will be convenient to use the following abbreviations:

$$\begin{aligned} m=m_\alpha&=\alpha\alpha_1+\beta\beta_1+\ldots+\lambda\lambda_1, \\ m_\beta&=(\alpha+\beta)\beta_1+\ldots+\lambda\lambda_1, \\ &\ldots\ldots\ldots\ldots\ldots\ldots, \\ m_\lambda&=(\alpha+\beta+\ldots+\lambda)\lambda_1. \end{aligned}$$

The orders of the groups generated by all the operators of G whose orders divide p^{α_1}, p^{β_1}, $\ldots$, p^{λ_1} are evidently p^{m_α}, p^{m_β}, $\ldots$, p^{m_λ} respectively.

To determine the value of m' we observe that G has a series of invariant subgroups of orders $p, p^2, \ldots, p^{m-1}$ under the given Sylow subgroup of order $p^{m'}$ in its group of isomorphisms. If we represent this series of invariant subgroups as follows:

$$H_1, H_2, \ldots, H_{m-1},$$

it is clear that H_1 is any one of the subgroups of order p generated by an independent generator of highest order. In fact, $H_1, H_2, \ldots, H_\alpha$ are generated respectively by $1, 2, \ldots, \alpha$ such subgroups. The subgroup $H_{\alpha+1}$ is generated by H_α and the subgroup of order p generated by an arbitary independent generator of order p^{β_1}, while $H_{\alpha+\beta}$ is the subgroup generated by the operators of order p in the subgroup of G generated by its independent generators of orders p^{α_1} and p^{β_1}. In general, $H_1, H_2, \ldots, H_{m-1}$ is a series of subgroups such that each is included in all those which follow it, but a characteristic subgroup of G is not always in this series. A subgroup in the given series which involves operators of order p^k must succeed every subgroup in this series which does not involve any operators of this order.

By means of the given notation it is easy to obtain the following formula:

$$\begin{aligned} m'&=m_\alpha-1+m_\alpha-2+\ldots+m_\alpha-\alpha+m_\beta-1+m_\beta-2+\ldots+m_\beta-\beta \\ &\qquad+m_\gamma-1+\ldots+m_\gamma-\gamma+\ldots+m_\lambda-1+\ldots+m_\lambda-\lambda \\ &=\alpha m_\alpha-\frac{\alpha(\alpha+1)}{2}+\beta m_\beta-\frac{\beta(\beta+1)}{2}+\ldots+\lambda m_\lambda-\frac{\lambda(\lambda+1)}{2} \\ &=\alpha^2\alpha_1+(2\alpha\beta+\beta^2)\beta_1+\ldots+(2\alpha\lambda+2\beta\lambda+\ldots+\lambda^2)\lambda_1 \\ &\qquad-\left(\frac{\alpha(\alpha+1)}{2}+\frac{\beta(\beta+1)}{2}+\ldots+\frac{\lambda(\lambda+1)}{2}\right). \end{aligned}$$

This result may be expressed as follows: *If an abelian group of order p^m is generated by α independent generators of order p^{α_1}, β of order p^{β_1}, ..., λ of order p^{λ_1} $(\alpha_1>\beta_1>\ldots\ldots>\lambda_1)$, the order of a Sylow subgroup of its group of isomorphisms is $p^{m'}$, where*

$$m'=\alpha^2\alpha_1+(2\alpha\beta+\beta^2)\beta_1+\ldots\ldots+(2\alpha\lambda+2\beta\lambda+\ldots\ldots+\lambda^2)\lambda_1 -\left(\frac{\alpha(\alpha+1)}{2}+\frac{\beta(\beta+1)}{2}+\ldots\ldots+\frac{\lambda(\lambda+1)}{2}\right).$$

Let $P_{m'}$ represent this Sylow subgroup of order $p^{m'}$. It is clear that $P_{m'}$ can always be represented as a transitive substitution group of degree p^{m-1}, since one of the largest independent generators s of G is transformed into itself multiplied by each of the operators of a subgroup of order p^{m-1} under $P_{m'}$, and G is generated by this subgroup and s. The regular subgroup R of $P_{m'}$, when $P_{m'}$ is represented as such a substitution group, which is formed by all the substitutions of $P_{m'}$ which are commutative with each of the independent generators of G except s, is of especial interest.

Let r_1 and r_2 be any two substitutions of R. Since all the operators of G may be written in the form ts^a, where t is an operator in the group generated by all the independent generators of G with the exception of s, it results that

$$r_1^{-1}sr_1=t_1s^{\alpha-1}s,\quad r_2^{-1}sr_2=t_2s^{\beta-1}s,$$

where t_1 and t_2 are commutative with both r_1 and r_2, and both $\alpha-1$ and $\beta-1$ are divisible by p. From the equations

$$r_1^{-1}s^{1-\beta}r_1s^{\beta-1}=t_1^{1-\beta}s^{\alpha-\alpha\beta+\beta-1},\quad r_2^{-1}s^{1-\alpha}r_2s^{\alpha-1}=t_2^{1-\alpha}s^{\alpha-\alpha\beta+\beta-1}$$

it results that the abelian subgroup of R generated by those substitutions for which $\alpha=\beta=1$ is a maximal abelian subgroup of R whenever G has more than one largest invariant. That is, it is not contained in a larger abelian subgroup of R whenever G contains more than one independent generator whose order is equal to the order of s.

If G contains only one independent generator of highest order and if the quotient obtained by dividing the order of s by the order of an independent generator of next to the highest order is p^γ, then r_1 and r_2 are commutative whenever α and β are such that both $\alpha-1$ and $\beta-1$ are divisible by the order of a generator of next to the highest order. The order of a maximal abelian subgroup of R in this case is therefore p^γ times the order of the subgroup formed by all the substitutions of R for which $\alpha=\beta=1$, provided G is non-cyclic. This completes a proof of the following theorem: *A necessary and sufficient condition that the subgroup R of order p^{m-1} be abelian is that G involves not more than one independent generator whose order exceeds p.*

As the subgroup R is invariant under $P_{m'}$, it results that $P_{m'}$ is contained in the holomorph of R. When R is abelian its invariants are the same as the invariants of G, with the exception that the largest invariant of G must be divided by p to obtain the corresponding invariant of R. In this case R is clearly a maximal abelian subgroup of $P_{m'}$, since $P_{m'}$ is always contained in the holomorph of R. A necessary and sufficient condition that $P_{m'}$ be a Sylow subgroup of the holomorph of R, when R is abelian, is that all the invariants of R are equal to p. As an illustrative example we may cite the fact that the group of degree 8 and order 1344 is the holomorph of R when G is the abelian group of order 16 and of type (1, 1, 1, 1). In this case $P_{m'}$ is a Sylow subgroup of order 64 contained in the given group of order 1344.

Another important invariant subgroup of $P_{m'}$ is composed of all the operators of I which transform each operator of G into itself multiplied by an operator of its subgroup of order p which is invariant under $P_{m'}$. In the given representation of $P_{m'}$ this subgroup must clearly have p^{m-2} transitive constituents of degree p, and its order is p^δ, δ being the number of invariants of G if at least one of these invariants exceeds p. If all these invariants are equal to p, then δ is one less than the number of invariants of G; that is, the order of the given invariant subgroup is p^{m-1} in this case. This result is a direct consequence of the important theorem that every abelian group has exactly as many subgroups of index p as it has subgroups of order p. A necessary and sufficient condition that the given invariant subgroup be a maximal abelian subgroup under $P_{m'}$ is that G involves no invariant that is divisible by p^3 and no more than one that is divisible by p^2.

As a very special case of what precedes we have the theorem: *A necessary and sufficient condition that a Sylow subgroup of order $p^{m'}$ of the group of isomorphisms of an abelian group of order p^m, $m>2$, be abelian, is that this group of order p^m is cyclic.* When no two invariants of G are equal to each other, the given series of invariant subgroups $H_1, H_2, \ldots, H_{m-1}$ is completely determined by G. On the other hand, this series is not completely determined by G whenever G has two equal invariants. As each such series corresponds to a Sylow subgroup in the group of isomorphisms of G, we have the following theorem: *A necessary and sufficient condition that the group of isomorphisms of an abelian group of order p^m must contain only one Sylow subgroup of order $p^{m'}$ is that this group of order p^m does not contain two equal invariants.**

The subgroup of G which corresponds to a particular operator of $P_{m'}$ has always an order which divides p^{m-1}. When G is cyclic, this order is evidently

* American Journal of Mathematics, Vol. XXVII (1905), p. 15.

p^{m-1} for some operator of $P_{m'}$. Suppose that G contains two different invariants and that the order of the larger exceeds p^2. It is clear that such a G contains a characteristic subgroup which involves operators of order p^2 without involving all the operators of order p contained in G. Hence there is no operator in a Sylow subgroup of order $p^{m'}$ of the group of isomorphisms of such a G, which corresponds to a subgroup of order p^{m-1} in G. In fact, such a correspondence implies that every two characteristic subgroups of G must have the property that one of them is contained in the other.